

CLAIMS

1. A processor-based electronic device, comprising:
a central processing unit (“CPU”);
a system memory device coupled to the CPU;
a decryption engine coupled to the CPU, the decryption engine being operable to perform a decrypting function;

an integrated circuit package housing the CPU, the system memory device and the decryption engine so that interconnections between the CPU, the system memory device and the decryption engine are inaccessible from outside the package; and

a source of a program in encrypted form, the source being external to the integrated circuit package and being coupled to the decryption engine, the encrypted program being decrypted by the decryption engine to allow the CPU to execute the program in unencrypted form.

2. The electronic device of claim 1 wherein the CPU, the system memory device and the decryption engine are fabricated as an integrated circuit on a common semiconductor substrate.

3. The electronic device of claim 1 wherein the decryption engine comprises a hardware decryption engine.

4. The electronic device of claim 1 wherein the decryption engine comprises a software decryption engine.

5. The electronic device of claim 4 wherein the decryption engine comprises:
a key storage device storing a decryption key; and

a decryption program storage device storing a decryption program that is executed by the CPU using the decryption key stored in the key storage device to decrypt the encrypted program stored in the non-volatile memory device.

6. The electronic device of claim 1 wherein the system memory device comprises a dynamic random access memory device.

7. The electronic device of claim 1, further comprising a system controller coupled between the CPU and the system memory and between the CPU and the non-volatile memory device, the system controller being housed in the integrated circuit package.

8. The electronic device of claim 1 wherein the decryption engine comprises:
a key storage device storing a decryption key; and
a decryption engine unit using the decryption key stored in the key storage device to decrypt the encrypted program stored in the non-volatile memory device.

9. The electronic device of claim 1 wherein the source of a program in encrypted form comprises a non-volatile memory device coupled to the decryption engine from outside the integrated circuit package, the non-volatile memory device storing the program in encrypted form.

10. The electronic device of claim 9 wherein the non-volatile memory device comprises a read-only memory device.

11. The electronic device of claim 9 wherein the non-volatile memory device comprises a flash memory device.

12. The electronic device of claim 9 wherein the non-volatile memory device comprises a mass storage device.

13. A secure processor module, comprising:

- a central processing unit (“CPU”);
- a system memory device coupled to the CPU;
- a decryption engine coupled to the CPU, the decryption engine being operable to perform a decrypting function; and

an integrated circuit package housing the CPU, the system memory device and the decryption engine so that interconnections between the CPU, the system memory device and the decryption engine are inaccessible from outside the package.

14. The secure processor module of claim 13 wherein the CPU, the system memory device and the decryption engine are fabricated as an integrated circuit on a common semiconductor substrate.

15. The secure processor module of claim 13 wherein the decryption engine comprises a hardware decryption engine.

16. The secure processor module of claim 13 wherein the decryption engine comprises a software decryption engine.

17. The secure processor module of claim 16 wherein the decryption engine comprises:

- a key storage device storing a decryption key; and
- a decryption program storage device storing a decryption program that is executed by the CPU using the decryption key stored in the key storage device.

18. The secure processor module of claim 13 wherein the system memory device comprises a dynamic random access memory device.

19. The secure processor module of claim 13, further comprising a system controller coupled between the CPU and the system memory and between the CPU and the non-volatile memory device, the system controller being housed in the integrated circuit package.

20. The secure processor module of claim 13 wherein the decryption engine comprises:

a key storage device storing a decryption key; and
a decryption engine unit using the decryption key stored in the key storage device to perform a decrypting function.

21. The secure processor module of claim 13 further comprising a data path coupled to the decryption engine from outside the integrated circuit package, the data path being adapted to couple a program in encrypted form to allow the decryption engine to decrypt the encrypted program thereby allowing the CPU to execute the program in decrypted form.

22. The secure processor module of claim 21 wherein the decryption engine is further operable to pass a request for the encrypted program through the data path.

23. A processor-based electronic device, comprising:
an integrated circuit package;
a CPU housed within the integrated circuit package;
a system memory device housed within the integrated circuit package;
an external interface circuit housed within the integrated circuit package;

a first plurality of conductors coupling the CPU to the system memory device and to the external interface circuit, the first plurality of conductors being housed within the integrated circuit package and being inaccessible from outside the integrated circuit package;

a second plurality of conductors coupled to the external interface circuit, at least some of the second plurality of conductors extending outside the integrated circuit package so that the conductors are accessible from outside the integrated circuit package; and

a source of a program in encrypted form, the source being external to the integrated circuit package and being coupled to at least some of the second plurality of conductors that extend outside the integrated circuit package.

24. The electronic device of claim 23 further comprising a non-volatile memory device located outside the integrated circuit package, the non-volatile memory device being coupled to at least some of the second plurality of conductors.

25. The electronic device of claim 24 wherein the non-volatile memory device stores a program that is executed by the CPU.

26. The electronic device of claim 23 wherein the CPU, the system memory device and the external interface circuit are fabricated as an integrated circuit on a common semiconductor substrate.

27. The electronic device of claim 23 wherein the external interface circuit comprises a system controller coupled between the CPU and the system memory.

28. The electronic device of claim 23 wherein the system memory device comprises a dynamic random access memory device.

29. The electronic device of claim 23 wherein the source of a program in encrypted form comprises a non-volatile memory device external to the integrated circuit package and coupled to at least some of the second plurality of conductors that extend outside the integrated circuit package.

30. A method of securely executing a computer program in a processor-based electronic device having a central processing unit (“CPU”), a system memory, and an external interface circuit, the method comprising:

- encrypting a computer program that is to be executed by the CPU;
- coupling the computer program to the external interface device;
- decrypting the computer program after the computer program has been coupled to the external interface device, the computer program being shielded from access after being decrypted;
- executing the decrypted computer program using the CPU; and
- during the execution of the computer program, coupling data between the CPU and the system memory, the data being shielded from access while being coupled between the CPU and the system memory.

31. The method of claim 30 wherein the act of shielding the data from access while the data are being coupled between the CPU and the system memory comprises packaging the CPU and the system memory in the same integrated circuit package.

32. The method of claim 30 wherein the act of shielding the data from access while the data are being coupled between the CPU and the system memory comprises fabricating the CPU and the system memory in the same integrated circuit substrate.

33. The method of claim 30 wherein the act of decrypting the computer program after the computer program has been coupled to the external interface device comprises:

storing a decryption key in a key storage device;
coupling the decryption key from the key storage device to a decryption engine;
coupling the computer program from the external interface device to the decryption engine;

using the decryption engine to decrypt the computer program based on the decryption key.

34. The method of claim 33 wherein the act of shielding the computer program from access after the program is decrypted comprises packaging the CPU, the key storage device and the decryption engine in the same integrated circuit package.

35. The method of claim 33 wherein the act of shielding the computer program from access after the program is decrypted comprises fabricating the CPU, the key storage device and the decryption engine in the same integrated circuit substrate.

36. The method of claim 30 wherein the act of executing the decrypted computer program using the CPU comprises:

after being decrypted, storing the decrypted computer program in the system memory; and

using the CPU to execute the computer program stored in the system memory by transferring the computer program from the system memory to the CPU for execution by the CPU.

37. The method of claim 30 wherein the act of executing the decrypted computer program using the CPU comprises transferring the decrypted computer program to the CPU for execution by the CPU after each as each of a plurality of program instructions are transferred from the program storage device.

38. The method of claim 30 wherein the act of decrypting the computer program after the computer program has been coupled to the external interface device comprises using the CPU to execute a decryption program that decrypts the computer program transferred from the program storage device.

39. The method of claim 30 wherein the processor-based electronic device further comprises a program storage device, and wherein the act of coupling the computer program to the external interface device comprises:

storing the computer program in the program storage device; and
coupling the computer program from the program storage device to the external interface device.